PAKE Combiners and Efficient Post-Quantum Instantiations

Julia Hesse*
IBM Research Europe – Zurich
juliahesse2@gmail.com

Michael Rosenberg
Cloudflare Research
michael@mrosenberg.pub

Version 1.0, October 10, 2024

Abstract

Much work has been done recently on developing password-authenticated key exchange (PAKE) mechanisms with post-quantum security. However, modern guidance recommends the use of *hybrid* schemes—schemes which rely on the combined hardness of a post-quantum assumption, e.g., Learning with Errors (LWE), and a more traditional assumption, e.g., decisional Diffie-Hellman. To date, there is no known hybrid PAKE construction, let alone a general method for achieving such.

In this paper, we present two efficient PAKE combiners—algorithms that take two PAKEs satisfying mild assumptions, and output a third PAKE with combined security properties—and prove these combiners secure in the Universal Composability (UC) model. Our sequential combiner, instantiated with efficient existing PAKEs such as CPace (built on Diffie-Hellman-type assumptions) and CHIC[ML-KEM] (built on the Module LWE assumption), yields the first known hybrid PAKE.

Keywords: key agreement, password-based cryptography, post-quantum cryptography

1 Introduction

Memorable passwords are the one of most commonly used forms of authentication today, and exist across a wide variety of applications. While some applications, such as website login, have users send their plaintext password, many large-scale applications utilize password-authenticated key exchange (PAKE) and its variants to limit the amount of information that can be intercepted. These include iCloud Keychain escrow, 1Password user authentication, Facebook Messenger chat history sharing, WhatsApp backup encryption, and passport chip access control [fan24].

*The author was supported by the Swiss National Science Foundation (SNSF) under the AMBIZIONE grant "Cryptographic Protocols for Human Authentication and the IoT".